Approved by Board 4/23/09

Policy on Participating Health Care Provider Policies and Procedures for the VHIE

Definitions –

"Consent" means an individual's act of giving permission to a Participating Health Care Provider in the Vermont Health Information Exchange ("VHIE" or "Exchange") to make the individual's protected health information ("PHI") available on the Exchange to, or to permit access to it by Participating Health Care Providers who are also involved in the treatment of the individual.

"Health Care Operations" shall mean activities of a Participating Health Care Provider providing treatment to an individual relating to quality assessment and improvement, evaluations relating to the competence of treating providers or necessary administrative and management activities all as defined in the HIPAA Privacy Regulations, 45 CFR §164.501.

A "Participating Health Care Provider" shall mean a health care provider, including any health care organization, that has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Treatment" shall mean the provision, coordination, or management of health care and related services by one or more health care providers.

Policy –

1. Each Participating Health Care Provider shall, at all times, comply with all applicable federal and state laws and regulations, including, but not limited to those protecting the confidentiality and security of protected health information ("PHI") and establishing individual privacy rights. Each Participating Health Care Provider shall comply with changes or updates to interpretations of such law and regulations to ensure compliance. Each Participating Health Care Provider shall update its Notice of Privacy Practices to describe its participation in the Exchange when an individual has consented to opt in and make his or her PHI available on the Exchange. Participating Health Care Providers shall be aware of the provisions of certain state laws, for instance, the Vermont patient privilege, 12 VSA §1612, which are more stringent than, and not preempted by, the HIPAA Privacy and Security Regulations. No Participating Health Care Provider shall permit access to PHI from the VHIE for purposes other than treatment, payment for treatment or necessary Health Care Operations without patient authorization, a court order or express requirement of law.

2. Each Participating Health Care Provider shall, at all times, comply with all applicable Exchange policies and procedures ("VHIE Policies"). These VHIE Policies may be revised and updated from time to time upon reasonable written notice to all Participating Health Care Providers. Each Participating Health Care Provider is responsible for ensuring it has, and is in compliance with, the most recent version of these VHIE Policies.

3. Each Participating Health Care Provider is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and VHIE Policies, including, without limitation, a sanctions policy. In the event of a conflict between VHIE Policies and Participating Health Care Provider's own policies and procedures, the Participating Health Care Provider shall comply with the policy that is more protective of individual privacy and security. Participating Health Care Provider shall enforce its policies and procedures by appropriately sanctioning individuals within its workforce and staff who violate its policies, VHIE Policies, or federal or state law.

4. Each Participating Health Care Provider shall have policies and procedures to promote the integrity of the PHI it maintains and makes available to the VHIE and the accuracy, relevance and completeness of such PHI. In the event PHI is amended either at the request of the Individual pursuant to the HIPAA privacy regulations or Vermont law or to otherwise correct inaccuracies, the Participating Health Care Provider making the amendment shall notify the VHIE and other Participating Health Care Providers who have accessed such PHI of such amendments.

5. Each Participating Health Care Provider shall designate individuals who may access the VHIE to retrieve PHI for the treatment of patients. With regard to its designated workforce or staff members, the policies of the Participating Health Care Provider shall require that they:

i. have or receive training regarding the confidentiality of PHI under the HIPAA Privacy and Security Regulation and all other applicable federal and state laws and they are obligated to protect PHI in compliance with such laws and VHIE Policies;

ii only access the Exchange for purposes of treatment of an individual or necessary health care operations;

iii hold any passwords, or other means for accessing the Exchange, in a confidential manner and to release them to no other individual;

iv comply with both VHIE Policies and those of the Participating Health Care Provider and that their workforce and staff members understand that their failure to do so may result in

their exclusion from the Exchange and may constitute cause for disciplinary action.

6. Each Participating Health Care Provider shall include in its policies and procedures that an individual shall not be denied treatment on the basis that he or she chooses not to consent to make his or her PHI available to the VHIE or who refuses to provide consent to the access by a Participating Health Care Provider to PHI made available by the individual to the VHIE.

Policy on Patient Consent to Opt In to VHIE

Definitions

"Consent" shall mean an individual's act of giving permission to a Participating Health Care Provider in the Vermont Health Information Exchange ("VHIE" or "Exchange") to make the individual's protected health information ("PHI") available on the Exchange to, or to permit access to it by, Participating Health Care Providers who are also involved in the treatment of the individual.

"De-identified" shall mean that all identifying information related to an individual as set forth in the HIPAA Privacy and Security Rule, 45 CFR § 164.514(b), are removed from the protected health information.

"Health Care Operations" shall mean activities of a Participating Health Care Provider providing treatment to an individual relating to quality assessment and improvement, evaluations relating to the competence of treating providers or necessary administrative and management activities all as defined in the HIPAA Privacy Regulations, 45 CFR §164.501.

A "Participating Health Care Provider" shall mean a health care provider, including any health care organization, that has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Protected Health Information" ("PHI") shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR §160.103.

"Treatment" shall mean the provision, coordination, or management of health care and related services by one or more health care providers.

Policy

Consent to Opt In

No protected health information ("PHI") of any individual shall be made available over the Exchange unless the individual has specifically consented in writing to make his or her PHI available to treating Participating Health Care Providers on the Exchange for the purposes of treatment, payment for treatment and health care operations. VITL shall only make available on the Exchange the PHI of individuals who have a current written consent for such availability on record.

The individual shall be provided educational information from VITL regarding the Exchange and its use by Participating Health Care Providers for treatment purposes. This information shall advise individuals of the ability of Participating Health Care Providers to access their PHI for treatment and also that VITL will

provide individuals with the ability to direct access to their PHI to Participating Health Care Providers if they consent to make their PHI available on the Exchange. It also shall advise them that their information can be available to Participating Health Care Providers providing treatment in an emergency and that de-identified information may be used for research, quality improvement and public health purposes. The individual shall be provided a Notice of Privacy Practices by the Participating Health Care Providers, as well.

Consent to access or to make PHI available on the Exchange may be revoked pursuant to the Participating Health Care Provider's Procedures as set forth in its Notice of Privacy Practices. The Participating Health Care Provider will promptly notify VITL in the event that an individual has revoked consent for his or her PHI to be available on the Exchange.

Consent to Opt In Procedure

VITL shall provide educational materials about the Exchange to Participating Health Care Providers, who shall make it available to patients. Participating Health Care Providers shall seek written or digital consent from patients to opt in and participate in the Exchange, and if consent to opt in is obtained, either enter that consent into their electronic health records system, which will then automatically notify the Exchange that the patient has opted in, or send the written consent form to VITL to enter with the Exchange. Participating Health Care Providers who include drug or alcohol treatment programs will specify an expiration date for the consents obtained from their patients. VITL shall establish a mechanism for Participating Health Care Providers to confirm that an individual has consented to opt in and shall facilitate the renewal of consents which have expiration dates.

Form of Consent to Opt In

An individual's consent to opt in to participate in the Exchange (1) shall be in writing, (2) shall be effective indefinitely unless it specifies an expiration date or is revoked and (3) shall include statements substantially similar to the following:

- I give my consent to all Participating Health Care Providers involved in my health care, including mental health, and substance abuse treatment providers, to access and use or disclose my protected health information to the Exchange for my treatment, for payment for my treatment and for health care operations consistent with the federal HIPAA privacy regulations and Vermont law.
- I consent to the disclosure of my protected health information by my Participating Health Care Provider electronically through the Exchange to any health care providers, including mental health and substance abuse treatment providers, for the purpose of my treatment, and I understand that I may direct that my Participating Health Care Providers obtain access to my protected health information on the Exchange.
- My consent includes the re-disclosure of protected health information received from a drug or alcohol treatment program for my treatment.

- I have received information from VITL regarding the Exchange and am aware that the privacy practices of my Participating Health Care Provider are described in its Notice of Privacy Practices.
- I am aware that de-identified information taken from my protected health information may be used for research, quality improvement and public health purposes.
- This consent is subject to my revocation/termination at any time except to the extent it has already been accessed by Participating Health Care Providers, including the inclusion of my information from the Exchange in the records of Participating Health Care Providers who are providing treatment to me.
- My consent is effective indefinitely unless either it relates to PHI from a drug or alcohol treatment program, or I choose to revoke or terminate my consent at an earlier date.
- I understand that I will be notified no less than once every five years of my right to revoke my consent.

Consent may be given in writing by an Individual's legal Representative as authorized by law.

Notification of Individual's Right to Revoke Consent

No less than once every five years, VITL shall notify and remind individuals who have consented to have their PHI accessible over the Exchange of his or her consent and of his or her right to revoke consent.

Individual Access to PHI on Exchange

An individual shall be provided the right of access to his or her PHI available on the Exchange through his or her Participating Health Care Provider or through VITL on behalf of a Participating Health Care Provider where so arranged. Individuals may direct that certain Participating Health Care Providers obtain access to his or her protected health information on the Exchange in addition to any Participating Health Care Providers being able to access the PHI for treatment of that individual.

Access by Treating Participating Health Care Providers Only

All Participating Health Care Providers on the Exchange shall have policies and procedures to ensure that only those involved in the diagnosis or treatment of an individual, payment for that treatment or necessary health care operations may access the individual's PHI on the Exchange. Participating Health Care Providers shall comply with the HITECH Act of 2009 and HIPAA privacy and security rule and all applicable state laws.

Re-disclosure Prohibition Notice

The Exchange shall provide notification to Participating Health Care Providers who access PHI on the Exchange substantially similar to the following statements:

- Information disclosed to you on the Exchange may include PHI received from a drug or alcohol treatment program protected by

Federal confidentiality rules, 42 CFR Part 2, which prohibit you from making further disclosure unless it is expressly permitted by a specific written consent from the subject individual or as otherwise permitted by the Rule. The Federal rules restrict use of information protected under 42 CFR Part 2 from criminal investigations or prosecutions of an alcohol or drug abuse patient.

Patient Request for Audit Report

An individual may request an Audit Report of access to his or her PHI on the Exchange by contacting VITL's Privacy Officer. VITL shall provide the requested Audit Report within 10 calendar days.

Revocation

An individual who has signed a written consent to permit his or her PHI to be available on the Exchange for treatment purposes shall be entitled to revoke such consent by providing written notice of revocation to VITL or to a Participating Health Care Provider with whom he or she has a provider/patient relationship. The Participating Health Care Provider shall promptly forward any such written notice of revocation to VITL. VITL shall effect such revocation of an individual's consent to opt in to the Exchange no later that 5 business days after receiving the notice of revocation.

Policy on Secondary Use of Identifiable PHI on VHIE

Definitions:

"Authorization" shall mean an individual's act of giving specific written permission for the use or disclosure of his or her protected health information in a form which meets all of the requirements set forth in the HIPAA Privacy Regulations, 45 CFR § 164.508.

"*De-identified*" shall mean that all identifying information related to an individual as set forth in the HIPAA Privacy and Security Rule, 45 CFR Section 164.514 (b), are removed from the protected health information.

"Health Care Operations" shall mean activities of a Participating Health Care Provider providing treatment to an individual relating to quality assessment and improvement, evaluations relating to the competence of treating providers or necessary management and administrative activities all as defined in the HIPAA Privacy Regulations, 45 CFR §164.501.

A "Participating Health Care Provider" means a health care provider, including any health care organization, who has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Protected Health Information" ("PHI") shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR § 160.103.

"Treatment" shall mean the provision, coordination, or management of health care and related services by one or more health care providers.

Policy

Identifiable protected health information ("PHI") shall not be made available on the Exchange for any purposes other than the treatment of the subject individual, payment related to that treatment or necessary health care operations of the Participating Health Care Provider who accesses PHI for treatment purposes. Consequently, *Identifiable* PHI on the Exchange shall not be made available by VITL without the patient's specific authorization:

- To any insurance carrier or other third party payer for payment or any purpose;
- To an employer for any purpose, unless the employer is a Participating Health Care Provider providing

treatment to the individual, and the individual has provided consent to opt in to the Exchange;

- To anyone for the purpose of marketing products or services or for any other commercial purpose;
- To anyone for the purpose of research; or
- To any member of law enforcement without a court order or express requirement of law.

De-identified PHI

In the event that *de-identified* PHI is requested for clinical research from data maintained for the Exchange, VITL, through its Executive Committee, or its designee Committee, shall review the request to determine if it should by approved. In making its determination, the Committee may consider any Institutional Review Board approval supporting the request. If approved, VITL, through an approved Data Subcontractor, shall prepare the *de-identified* PHI requested and shall be reimbursed for its expenses by the requesting party. The requesting party shall be required to provide contract assurances that no attempt shall be made by it to "identify" the *de-identified* PHI from the Exchange provided for the approved research.

VITL shall make available upon request an annual report of all approved requests for de-identified PHI from the Exchange, including the date of the de-identified data release, the entity to which the data was released, and a summary of the research involved.

Policy on Information Security

Definitions

The "Vermont Health Information Exchange" ("VHIE") shall mean the health information exchange network operated by VITL.

A "Participating Health Care Provider" shall mean a health care provider, including any health care organization, that has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Protected Health Information" ("PHI") shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR §160.103.

"Technical safeguards" shall mean "the technology and the policy and procedures for its use that protect electronic PHI and control access to it."

Policy

Policy Overview

The purpose of the VITL Information Security Policy is to ensure that appropriate technical, administrative, and physical safeguards are applied end-to-end in the VHIE, including VITL and participating providers. The policy draws upon industry-standard guidelines such as HIPAA Security Guidance and International Organization for Standardization (ISO) security practices. For VITL, the policy requires independent certification of security best practices at the "core" of the exchange. For Participating Health Care Providers, the policy requires that providers affirm compliance with the HIPAA Security Rule, and recommends a risk assessment process based on HIPAA requirements that allows providers to demonstrate the application of specific safeguards most appropriate to their size and function. End-to-end compliance with security practices is also enhanced by VITL-provided training, guidance, and technologies for automated compliance.

Ensuring Security of the Core Infrastructure

In a health information exchange, the core infrastructure includes the systems and personnel to operate the components at the center of the network. The core infrastructure shall be certified for compliance by at least one independent certifier of industry standard information security practices, such as the Electronic Healthcare Network Accreditation Commission (EHNAC). EHNAC is an independent, non-profit accrediting agency that evaluates an organization's ability to meet standards and best practices. EHNAC certification includes a rigorous set of requirements aimed at HIPAA transaction processors, clearinghouses, and data centers, in the areas of Privacy and Confidentiality, Technical Performance, Resources, and HIPAA

Security. VITL shall publish and maintain core infrastructure certification information on its website.

Ensuring Security at the Participating Health Care Providers

Participating Health Care Providers, as HIPAA covered entities, must comply with HIPAA Security rules and HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information. This requires HIPAA Security practices to mitigate risk in three areas: Accessing Health Information, Storing Health Information, and Transmitting Health Information. Participating providers shall affirm compliance with the HIPAA Security Rule, including eight HIPAA-based practices listed in the Risk Assessment subsection below. VITL reserves the right to conduct a security audit of participating providers to demonstrate compliance.

Risk Assessment

Participating Health Care Providers are required by HIPAA Security Rule §164.308 (a)(ii)(A) to conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic PHI. Based on the HIPAA requirements and Security Guidance published by the Department of Health and Human Services, VITL recommends that the risk assessment should include, but not be limited to, the following practices across eight subject areas:

1. Security policy and organization. Each Participating Health Care Provider should designate a Privacy Officer and Security Officer, and maintain a written security policy made available to all personnel with access to PHI. Confidentiality agreements should be utilized for third-parties with PHI access. The Privacy Officer and Security Officer should hold regular meetings with the management of the organization. They should develop processes for writing incident reports, regularly reviewing logs, end-user management including account creation, and patient inquiries.

2. Asset management. Each Participating Health Care Provider should maintain an inventory of health information assets containing PHI or with access to PHI such as laptops, desktops, servers, and removable media. A custodian should be identified to maintain the inventory, and rules should be written into security policy for acceptable use of the assets.

3. Human resources. Each Participating Health Care Provider should consider the information security impacts for employees joining, moving and leaving the organization. Job descriptions should indicate who has responsibilities related to PHI, and contracts with employees and contractors should include reference to information security policies, including information security-related disciplinary procedures. The Participating Health Care Provider should have procedures for removing access to PHI upon termination of employment or contract. The

Participating Health Care Provider should promote information security awareness through education and training for employees.

4. Physical and environmental security. Each Participating Health Care Provider should take reasonable steps to protect computer facilities and equipment containing or with access to PHI. Depending on the size of the organization, this may include establishing secure areas and deploying physical security measures for these areas. Where IT equipment is used off-premises, the organization should have policies for remote use of laptops or home computers. Procedures for secure disposal of IT equipment should be followed.

5. Communications and operations management. Each Participating Health Care Provider should take responsibility for the management of technical security controls in its systems and networks that are used to access PHI. The Participating Health Care Provider or its contractors should have documented operating procedures and formal change control process for implementing changes to systems or networks. Controls to prevent, detect, and respond to malicious software and network intrusion should be deployed. When stored on portable media, PHI should be tracked, and encrypted or protected from theft. A secure audit log should be created whenever PHI is accessed, created, updated, or archived. The auditing should be implemented at all times, and procedures for analyzing audit logs should be followed.

6. Access control. Each Participating Health Care Provider should take measures to limit access to networks, systems, applications, functions and data to authorized personnel. An access control policy should be established including password management procedures.

7. Information systems acquisition, development and maintenance. The Participating Health Care Provider should take steps to ensure that security is built into EHR and other clinical systems that store electronic PHI.

8. Information security incident management. Each Participating Health Care Provider should anticipate and respond appropriately to privacy and security related events such as breaches. Policies should be established for response to such events.

Secure Audit Logs

In addition to the audit logs kept by the provider for its own records, VITL shall maintain a comprehensive set of audit logs detailing accesses to the exchange. VITL audit policies, as described in the Auditing and Access Monitoring Policy, include regular review of audit logs by the VITL Privacy Officer as well as delegated review of selected logs by the Participating Health Care Provider Privacy Officer. Procedures for follow-up on suspicious

activity, such as indications of possible privacy or security breaches, are described in the VITL Privacy and Security Events Policy.

Detailed Guidelines and Training

No security policy can be successfully implemented without a training component. The Participating Health Care Provider Privacy Officer will be required to attend an online security training session sponsored by VITL. All VHIE end-users must submit a written acknowledgement of security and privacy policies. VITL may also sponsor optional annual supplemental security training for all interested users.

In addition to this policy document, VITL shall periodically publish guidelines to assist with the implementation of the ISO best practices defined above.

Affinity Domain Policy

As described in the Vermont Health Information Technology Plan, the VHIE is designed to be compatible with the Integrating the Healthcare Enterprise (IHE) architecture. IHE provides technical frameworks for the use of existing standards, reducing variability in their implementation. The integration profiles that make up IHE technical frameworks specify how standards should be used to achieve specific needs within the framework.

VITL shall publish and maintain on its website a detailed IHE Affinity Domain Interoperability Policy Agreement which will include technical details for statewide standard interoperability requirements and specifications including standard content, identification schemes, vocabularies, actors, and transactions to be supported by the VHIE. These Cross-Enterprise Document Sharing (XDS) profile extensions are being defined statewide in Vermont and shall be followed by all VHIE participants within the state. They will include further details in the following areas related to technical security, including:

- Authorization
- Role Management
- Definition of Functional and Structure Roles
- Identity Management Policy and Authentication of Users
- Attestation and Delegation Policy
- Node Authentication Requirements

Technologies for Automated Compliance

VITL shall utilize technologies for automated compliance with security policies where practical. For example, VITL may implement an automated system which would require the existence of a current antivirus software on the end-user's terminal before access is granted to the exchange. VITL may employ automated intrusion detection systems, and may request that Participating Health Care Providers deploy similar software or participate in the application of these systems.

Procedures for Non-compliance

Procedures for non-compliance, including sanctions, are described in the Privacy and Security Events Policy.

Policy on Privacy and Security Events

Definitions

A "Reportable Event" is defined as an action (or lack of action) that violates VITL's policies and procedures for accessing or using protected health information on the Vermont Health Information Exchange. Such violations may be unintentional or intentional. Reportable events include any type of violation or breach involving the Vermont Health Information Exchange.

A "Breach" is defined as a Reportable Event involving the unauthorized acquisition, access, use or disclosure of protected health information on the Vermont Health Information Exchange which compromises the security or privacy of protected health information maintained by or on behalf of a person. Such term does not include a Reportable Event where an unauthorized person to whom such information is disclosed would not have reasonably been able to retain such information. Such term also does not include:

i. any unintentional acquisition, access or use of such information by an employee or agent of the Participating Health Care Provider or its business associate if such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or agent, respectively, with the Participating Health Care Provider or business associate and if such information is not further acquired, used, or disclosed by such employee or agent; or
ii. any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a Participating Health Care Provider or its business associate to another similarly situated individual within the same facility; and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

The following examples distinguish the above terms:

- An example of a Reportable Event is a clinician sharing his user name and password with another clinician in the practice who had forgotten his own user name and password, and the clinician using the borrowed user name and password to access the health information exchange. This is a Reportable Event because it violates VITL's privacy and security policies, which require each user to log in with their own authentication and will result in inaccurate audit logs and reports. It is not considered a Breach because the privacy of protected health information was not compromised, as the clinician who borrowed the user name and password was also authorized to access the patient information on the exchange.

- An example of a Breach is a hospital registration clerk stealing a clinician's user name and password to gain unauthorized access to the Vermont Health Information Exchange, and printing out the clinical summary of the clerk's mother-in-law. This is considered a Breach because there was an unauthorized disclosure of protected health information which compromised the privacy of data maintained on behalf of a person.

An "Unintentional Violation" is defined as a violation of policies, procedures or law without planning or forethought. The violation may have been accidental in nature or due to a lack of training or understanding of requirements.

An "intentional violation" is defined as a deliberate violation of policies, procedures or law, conducted with planning or forethought.

The "Vermont Health Information Exchange" ("VHIE") shall mean the health information exchange network operated by VITL.

A "Participating Health Care Provider" shall mean a health care provider that has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Protected Health Information" ("PHI") shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR § 160.103.

"Unsecured Protected Health Information" shall mean PHI that has not been secured through the use of a technology or methodology standard as provided by federal law.

Policy

Response to Reportable Events

Participating Health Care Providers are obligated to report all Reportable Events involving the Vermont Health Information Exchange that they are aware of to their organization's privacy and security officer(s), who will advise VITL of the Reported Event. VITL will establish and publicize one or more methods for filing reports.

Other individuals who have information about Reportable Events involving the Vermont Health Information Exchange are encouraged to file reports or complaints with VITL's privacy and security officer. VITL will establish and publicize one or more methods for members of the public who

have information about Reportable Events involving the Vermont Health Information Exchange to file complaints.

Upon receipt of a Reportable Event Report or Complaint, VITL's privacy and security officer will log the Reportable Event, acknowledge receipt of the Reportable Event report or complaint to the person who filed it, inform the affected Participating Health Care Provider's privacy and security officer(s) of the event if they do not already have knowledge of it, and begin a review of the event to the extent that it involves the VHIE. If it appears to VITL's privacy and security officer that there is an imminent threat to data security on the Vermont Health Information Exchange, VITL's privacy and security officer will take immediate actions to secure data.

The privacy and security officer(s) of the affected Participating Health Care Provider will cooperate with the Reportable Event review. Once the facts are gathered, VITL's privacy and security officer will determine whether a violation of VITL's privacy and security policies, procedures or relevant federal or state law has occurred.

VITL and the affected Participating Health Care Provider will collaborate to take steps to correct any weaknesses in their systems, policies, or procedures that were identified during the review. The privacy and security officer(s) of the affected Participating Health Care Provider will work with VITL's privacy and security officer to consider the need to develop a mitigation plan that is mutually acceptable. The mitigation plan should include steps to prevent the Reportable Event from reoccurring, and may include but not be limited to: additional employee training and education; facility and computer system changes; and policy revisions.

Upon completing the review, VITL's privacy and security officer will compile a final written report about the Reportable Event, communicating to the affected Participating Health Care Provider the facts gathered, the determinations made, any steps being taken to mitigate the event, and the measures being taken to prevent such an event from reoccurring. VITL's privacy and security officer will inform other complaint or report filers what actions were taken in response to the complaint/report. Whenever possible, this report will be in writing.

On a quarterly basis, VITL will conduct a review of all the events that occurred during the quarter to look for commonalities and opportunities for improvement. If any commonalities or opportunities for improvement are identified, VITL will take measures to address them. VITL will make a quarterly report summarizing the reportable events involving the health information exchange available to the Secretary of Administration or designee, including a trend analysis.

Upon request, VITL shall provide a report enumerating the warrants and subpoenas served upon it and/or the VHIE for data on the VHIE over the past twelve months. This report shall list the month and year the subpoena or warrant was issued, the issuing court, agency, or entity, and the individual or entity that caused the subpoena or warrant to issue and the status of the subpoena or warrant. Any subpoena or warrant issued at the behest of a non-government entity or individual shall be listed as being requested by a private party.

Breach Notification

In circumstances where it has been determined that a Reportable Event constitutes a Breach, VITL will notify the Participating Health Care Provider(s) whose patient information was subject to the unauthorized acquisition, access, use or disclosure no later than ten business days following the discovery of the Breach. Such notification will include the time and date of the Breach discovery and the identification of each individual whose PHI is involved.

The Participating Health Care Provider, and/or VITL at the Participating Health Care Provider's request, shall notify, without unreasonable delay and in no case later than 60 days from the discovery of the Breach, each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of the Breach. Notification shall be provided in writing to each affected individual, or next of kin if deceased, by first class mail, or, if specified by the individual, by electronic mail. Notice shall also be provided to the Secretary of the U.S. Department of Health and Human Services in the form of an annual breach log submission as required by the Secretary. If the affected Participating Health Care Provider or VITL concludes that there may be imminent misuse of an individual's PHI, notice shall also be provided by telephone contact or other means, as appropriate. If the unsecured PHI of more than 500 individuals is affected by a Breach, notice shall also be provided to prominent media outlets serving the area and immediately to the Secretary of U.S. Department of Health and Human Services.

In the case in which there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual, electronic) notification to the individual, a substitute form of notice shall be provided. In the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, the involved Participating Health Care Provider will provide notice by arranging for a conspicuous posting on the home pages of the Web site, if available, of the Participating Health Care Provider involved and of VITL and/or notice in major print or broadcast media where the individuals affected by the breach

likely reside. Such a notice in media or web postings will include a toll-free phone number to either the Participating Health Care Provider and/or VITL, as mutually agreed upon, where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

The notification to the affected individual(s) will contain, to the extent possible, the following:

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

2. A description of the types of unsecured protected health information that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code.)

3. The steps individuals should take to protect themselves from potential harm resulting from the Breach.

4. A brief description of what the Participating Health Care Provider and VITL are doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

If a law enforcement official determines that a notification required under this Policy would impede a criminal investigation or cause damage to national security, such notification shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under each section.

Mitigation, Corrective Action and Sanctions

Upon receiving a report or being notified of a reportable event, VITL will work with the affected Participating Health Care Provider(s) to develop a mutually acceptable mitigation and correction plan.

If it is determined by VITL's privacy and security officer that a reportable event or a breach has occurred involving the health information exchange, VITL may impose on the offender one or more sanctions, consistent with the violation. Depending on the circumstances, sanctions may be on an individual level or an organizational level. Sanctions for an unintentional violation may

include, but are not limited to: verbal warnings; written warnings; suspension of exchange access privileges; and revocation of exchange access privileges. Sanctions for an intentional violation may include, but are not limited to: immediate suspension of exchange access; revocation of exchange access; a complaint filed with the violator's professional licensing board, if the violator is professionally licensed; information turned over to a prosecutor for criminal prosecution; and potential other legal action.

Appeals

Offenders may appeal sanctions to VITL. All appeals must be filed in writing, and received at VITL's business offices within 10 business days of the sanction being imposed. VITL staff will consider the appeal and make a determination of whether to continue the sanction within 10 business days of receiving the written appeal. VITL will provide the party filing the appeal with a written notice of its decision within 10 business days of making the decision. Sanctions will remain in effect while the appeal is being considered.

If the appeal is denied, and the appealing party believes there has been an error, it may file a request with VITL for an external review. Such requests must be made in writing within 30 calendar days of the appeal being denied. VITL will refer the case to an independent party, which will review the evidence and make a recommendation to VITL's board of directors, which will make the final decision.

Policy on Auditing and Access Monitoring

Definitions

The "Vermont Health Information Exchange" ("VHIE") shall mean the health information exchange network operated by VITL.

A "Participating Health Care Provider" shall mean a health care provider that has executed an effective VHIE Data Services and Participation Agreement with VITL.

"Protected Health Information" ("PHI") shall mean identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual as defined in the HIPAA Privacy Regulations, 45 CFR §160.103.

"Unsecured Protected Health Information" means PHI that has not been secured through the use of a technology or methodology standard as provided by federal law.

"Audit" means an individual's act of reviewing and examining records of activity related to the records of access and use of the VHIE by participating health care providers.

"Audit Logs" means system generated reports based on logging and recording transactions sent and received, access records (including denied access), and other information related to tracking use and access by Participating Health Care Providers in the VHIE.

Policy

1. Audit logs shall be generated by the VHIE, by the Participating Health Care Providers' EHR systems, and by other computer software and systems that communicate with the VHIE to access, store and communicate personal health information about individuals who have opted in to the VHIE.

2. Audit logs accessible by Privacy Officers of Participating Health Care Providers shall be restricted to records of access by the Participating Health Care Provider.

3. VHIE Audit logs shall be reviewed on a routine basis by the VITL Privacy Officer and by the Privacy Officer of Participating Health Care Providers. Any suspicious activity discovered by VITL shall be reported to the Participating Health Care Provider and VITL shall generate a Reportable Event report. Any suspicious activity discovered by a Participating Health Care Provider shall be reported to VITL; VITL shall generate a Reportable

Event report as per the VITL Privacy and Security Events Policy. The VITL Privacy Officer shall specifically review audit logs to detect intrusion attempts and patterns of access to the VHIE.

4. VHIE Audit logs shall be reviewed by VITL and Participating Health Care Provider as needed to follow up on inquires from providers and patients regarding accesses and use of the VHIE.

5. As per the Policy on Information Security, Participating Health Care Providers are expected to create secure audit logs whenever PHI is accessed, created, updated, or archived via an EHR or other information system. Audit logging shall be implemented at all times and procedures for analyzing audit logs shall be provided and used by the provider.

VHIE Audit Logs

A secure audit log shall be created whenever PHI is accessed, created, updated, or archived via the exchange. Audit logging shall be implemented at all times, and procedures for analyzing audit trails shall be used by the VITL Privacy Officer and Participating Health Care Provider Privacy Officers.

VITL Privacy Officer and Participating Health Care Provider Privacy Officers shall be provided with facilities for analyzing logs and audit trails that:

- allow the identification of all VHIE users who have accessed or modified a given subject of care's PHI in the VHIE over a given period of time, and
- allow the identification of all subjects of care whose PHI has been accessed or modified by a given VHIE user over a given period of time.

Audit logs shall be secure and tamper-proof. Access to system audit log analyzing tools and audit logs shall be safeguarded to prevent misuse or compromise.

For transactions sent to or from the VHIE, the audit system shall record:

- sender identifier
- date and time of event
- system component where the event occurred
- type of event or transaction
- outcome of the event (success or failure)

For user access events, the audit system shall record:

- user identifier
- date and time of event

- system component where the event occurred
- type of event
- outcome of the event (success or failure)

For granting/revoking access to the VHIE the audit system shall record:

- user identifier
- date and time of event
- system component where the event occurred
- type of event (authorization, revocation, password change)
- outcome of the event

All access and transaction logs shall be kept for six years.

Patient Request for Audit Report

An individual may request an audit report of access to his or her PHI on the VHIE, for a period no longer than three years prior to the date of request, by contacting VITL's Privacy Officer. VITL shall provide the requested Audit Report within 30 calendar days, and it shall provide the following information pursuant to 45 CFR § 164.528(b):

1. The date of disclosure;

2. The name of the Participating Health Care Provider and/or user or other person who received the protected health information and, if known, the address of such entity or person;

3. A brief description of the protected health information disclosed; and

4. A brief statement of the purpose of the disclosure.